

A Methodological Approach for Trustworthiness Assessment and Prediction in Mobile Online Collaborative Learning

Jorge Miguel^{a,*}, Santi Caballé^a, Fatos Xhafa^a, Josep Prieto^a, Leonard Barolli^b

^a*Department of Computer Science, Multimedia, and Telecommunication, Open University of Catalonia, Barcelona, Spain*

^b*Fukuoka Institute of Technology, Department of Information and Communication Engineering, Fukuoka, Japan*

Abstract

Trustworthiness and technological security solutions are closely related to online collaborative learning and they can be combined with the aim of reaching information security requirements for e-Learning participants and designers. Moreover, mobile collaborative learning is an emerging educational model devoted to providing the learner with the ability to assimilate learning any time and anywhere. In this paper, we justify the need of trustworthiness models as a functional requirement devoted to improving information security. To this end, we propose a methodological approach to modelling trustworthiness in online collaborative learning. Our proposal sets out to build a theoretical approach with the aim to provide e-Learning designers and managers with guidelines for incorporating security into mobile online collaborative activities through trustworthiness assessment and prediction.

Keywords: information security, trustworthiness, assessment, prediction, online collaborative learning, mobile learning

1. Introduction

Over the last decade, Computer Supported Collaborative Learning (CSCL) has become one of the most influencing paradigms devoted to improving e-Learning [1]. Similarly, mobile learning is an emerging educational model devoted to providing the learner with the ability to assimilate learning any time and anywhere [2]. Mobile learning provides ubiquity and pervasiveness, which have become essential requirements to support learning and allow all learning community members from a variety of locations to cooperate with each other by means of a large variety of technological equipment [3]. While there has been an explosion of mobile devices and applications in the marketplace to gain access to e-Learning systems and collaborative learning processes, the development of mobile supported collaborative learning guided by technological security as a key and transverse factor has been, to the best of our knowledge, little investigated [4]. However, Information and Communication Technologies (ICT) have been widely adopted and exploited in most of educational institutions in order to support e-Learning through different learning methodologies, ICT solutions and design paradigms. In this context, e-Learning designers, managers, tutors, and students are increasingly demanding new requirements. Among these requirements, information security is a significant factor involved in e-Learning processes. However, according to [5, 6], e-Learning services are usually designed and implemented without much consideration of security aspects. This finding has been usually tackled with ICT security solutions, but as stated in [7], the problems encountered in ensuring modern computing systems, cannot be solved with ICT alone. In contrast, current advanced ICT security solutions are feasible in many e-Learning scenarios though assessment processes in CSCL involve specific non-technological components. Indeed, online assessment activities (e-assessment) usually have specific issues, such as student's grades or course certification, that e-Learning designers have to consider when they manage security requirements. In this context, even most advanced and comprehensive technological security solutions cannot cope with the whole domain of e-Learning vulnerabilities.

*Corresponding author

Email address: jmmoneo@uoc.edu (Jorge Miguel)

An e-Learning activity is a general concept that can involve very different cases, actors, processes, requirements, and learning objectives in the complex context of e-Learning [8]. To conduct our research we focus on specific online collaborative activities, namely, online assessment (e-assessment). In [9], the authors report that the e-assessment process offers enormous opportunities to enhance the student's learning experience, such as delivering on-demand tests, providing electronic assessment, and immediate feedback on tests. In this context, e-assessment is considered an e-exam with most common characteristics of virtual exams, and is typically employed to deliver formative tests to the students. An e-assessment activity is an e-exam with most common characteristics of virtual exams. Moreover, in [10] it is discussed how unethical conduct during e-learning exam-taking may occur and an approach that suggests practical solutions based on technological and biometrics user authentication is proposed.

In our real context of online higher education, we mainly consider peer-to-peer assessment processes and online collaborative activities, which will form e-assessment components. In this context, we propose security technological solutions extended with a functional trustworthiness approach [11, 12, 13] by proposing a hybrid assessment method based on trustworthiness models. From these previous works, in this paper, we endow trustworthiness models for security in e-Learning with a trustworthiness methodology. This approach is devoted to improving security in CSCL by building a trustworthiness methodology to offer guidelines for designing as well as managing security in online collaborative activities, through trustworthiness assessment and prediction. To this end, we propose a trustworthiness methodology with the aim of managing and predicting reliable assessment processes in e-assessment. As a result, by predicting collaborative e-assessment results, e-Learning designers will be able to manage assessment process with additional information generated by automatic prediction models.

This paper is structured as follows. In Section 2 we review the main works in the literature on mobile collaborative learning and security in CSCL, how trustworthiness assessment and prediction is related to security, and trustworthiness methodologies. In Section 3, we describe the theoretical features, phases, data, and processes of our methodological approach. In order to validate and support the application of the methodology, in Section 4 we concrete the most significant aspects in terms of specific methods through their application in real online courses. Moreover, in Section 5 we present and evaluate a neural network approach for peer-to-peer e-assessment prediction. Finally, conclusions and further work are presented in Section 6.

2. Background

In this section, we review the main works in the literature on mobile collaborative learning and security in collaborative learning, how trustworthiness assessment and prediction is related to security, and trustworthiness existing methodologies.

2.1. Security in Online Collaborative Learning

According to [1], Computer Supported Collaborative Learning has become one of the most influencing educational paradigms devoted to improving e-Learning. Some authors argued that information security has to be considered with the aim of ensuring information managed in CSCL. In addition, several technological solutions were proposed [5, 6]. These security solutions, based on technological approaches, tackle the security in e-Learning problem with specific methods and techniques that deal with particular security issues, but these models does not offer an overall security solution [14, 4]. One of the key strategies in information security is that security drawbacks cannot be solved with technology solutions alone [7]. Even most advances security ICT solutions have drawbacks that impede the development of complete security frameworks.

Finally, some authors argue we need to understand attacks in order to discover relevant security design factors [15]. Real-life security attacks and vulnerabilities are presented in many security reports, which justify the relevance of security attacks over the last years [16, 17].

2.2. Mobile Collaborative Learning

Mobile learning has lately emerged with the increasing use of mobile technology in education. According to [2] and [3] the needs of educational organizations are increasingly related to modern online learning environments which must provide advanced capability for the distribution of learning activities and the necessary functionalities and learning resources to all participants, regardless of where these participants and resources are located, and whether

this location is static or dynamic. The aim of newest learning environments is to enable the learning experience in open, dynamic, large-scale, and heterogeneous environments.

Although, from a general point of view, mobile learning can be considered as any time and anywhere learning experiences, [18] shows how we can consider multiple definitions of m-Learning. Moreover, because of the complexity and multidisciplinary factors of Mobile Computer Supported Collaborative Learning (MCSCCL) paradigm, in [3] a three-dimensional approach has been provided to understand and unify the rather dispersion currently existing in advanced learning practices and pedagogical goals from the era of MCSCCL. This approach considers the context of MCSCCL from a multiple dimensional perspective: pedagogical, technological and evaluation.

In this paper, we will focus mobile learning specially on the use of mobile devices (i.e. tablets or smart phones) when developing CSCL activities. In this sense, mobile learning educational process can be considered as any learning and teaching activity that is possible through mobile tools or in settings where mobile equipment is available [18]. Therefore, we consider mobile devices do not change significantly the CSCL processes and methodologies presented in the next sections. Hence, for the sake of simplicity, in the rest of the paper we will refer to online collaborative learning or CSCL only, which implicitly include MCSCCL and collaborative learning supported by mobile devices.

2.3. Trustworthiness Models and Normalization

According to [19], there is a degree of convergence on the definition of trustworthiness. This can be summarized as follows: trustworthiness is a particular level of the subjective probability with which an agent assesses that another agent (or group of agents) will perform a particular action, before the agent can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects its own action. Regarding trustworthiness and e-Learning, according to [20], a trustworthy e-Learning system is a learning system, which contains reliable serving peers and useful learning resources.

As stated by the authors in [21], through the study of the most relevant existing trust models, trustworthiness modelling can be classified into trustworthiness assessment and prediction models (note that in the literature on trustworthiness modelling, the terms determination and estimation are also used to refer assessment and prediction respectively). The first formally trustworthiness model related to information technology services was proposed in [22] from three levels. This approach considers the main factors and rules dealing with trustworthiness, which can be summarized as follows:

1. Basic trust is the general trusting disposition of an agent at time.
2. General trust represents the trust that agent has on other agent at time.
3. Situational trust is the amount of trust taking into account a specific situation.

It is worth mentioning that this early proposal takes into account the time factor (discussed in Section 2.5) as a key trustworthiness component in the model.

Although trustworthiness models can be defined and included as a service in e-assessment security frameworks, there are multiple issues related to trustworthiness, which cannot be managed without normalization [23]. Among these issues, we can highlight trustworthiness multiple sources, different data formats, measure techniques, and other trustworthiness issues, such as rules, evolution, or context. Hence, in [13], we justify why trustworthiness normalization is needed and a normalized trustworthiness model is proposed by reviewing existing normalization procedures for trustworthy values applied to e-assessments.

2.4. Trustworthiness and Information Security

To overcome security deficiencies discussed above, we researched into enhancing technological security models with functional approaches [11, 12, 13]. In [20], a trustworthy e-Learning system is defined as a learning system, which contains reliable serving peers and useful learning resources. As stated by the authors in [21], through the study of the most relevant existing trust models, trustworthiness modelling can be classified into trustworthiness assessment and prediction models. In this paper, we considered both purposes of trustworthiness. In addition, we also consider trustworthiness models, rules, factors and features that we discussed in [11, 12, 13] with the aim to enhance security in e-Learning through trustworthiness methods.

To establish the difference between assessment and prediction, in [21] it is stated that trustworthiness prediction, unlike trust assessment, deals with uncertainty as it aims to predict the trust value over a period in the future. In such cases, the accuracy of the trust values at a point in time in the future is an important issue to be considered, as the future of business decisions will be based on these.

2.5. Time Factor and Trustworthiness Sequences

Several studies investigating trustworthiness show that time factor is strongly related to trustworthiness [20, 24, 25]. The authors in [20] stated that trust is dynamic and will attenuate when time goes by. For instance, A trusts B at time t_0 , but A might not trust B in a follow-up time t_1 . In [23], it is presented the design and development of a trust management system. This system addresses its specifications and architecture to facilitate the system implementation through a module-oriented architecture. Among the modules of the system, the authors define a module for dynamic assessment, which includes trust levels assessment based on dynamic trust criteria. The module integrates assessment from all parts to calculate trust value by the weighted average.

As aforementioned, we can consider both assessment and prediction trustworthiness models. Although the models reviewed analysing trustworthiness include the time factor as a key component, we need further modelling techniques that allow us to conduct trustworthiness assessment towards prediction. To this end, we reviewed the concept of Trustworthiness History Sequence [25]. In the context of grid services, Trustworthy History Sequence is a history record of trustworthy of grid service that the requester has traded with. It can be denoted with an ordered tuple where each component is the trustworthy of the transaction between a requester and a service.

2.6. Predicting Trustworthiness

Trustworthiness predictions models, to the best of our knowledge, have been little investigated in the context of e-assessment, even in a general prediction scope. The existing literature suggests that the term trust prediction is used synonymously and interchangeably with the trust assessment process [21] presented in the sections above. Moreover, trustworthiness does not focus on an isolated technical application, but on the social context in which it is embedded. Although trustworthiness building can be supported by institutions, there is no easy way out [26]. In addition, the building of trust can be a very lengthy process, the outcome of which is very hard to predict.

Several studies investigating trustworthiness prediction were carried out with neural networks [21, 25, 27]. In [21], the authors propose the use of neural networks to predict the trust values for any given entities. The neural networks are considered one of the most reliable methods for predicting values [21]. A neural network can capture any type of non-linear relationship between input and output data through iterative training, which produces better prediction accuracy in any domain such as time series prediction. The key contribution of this work is focused on the dynamic nature of trust, in which the performance of this approach is tested under four different types of data sets (e.g. non-uniform stationary data, different size, etc.), and the optimal configuration of the neural network is identified.

In [25], the authors stated that trustworthiness prediction with the method of neural network is feasible. The experiments presented in [25] confirm that the methods with neural networks are effective to predict trustworthiness. This method is based on defining a neural network structure, a neural network constructing, an input standardization, a training sample constructing, and the procedure of predicting trustworthiness with trained neural network.

The work presented in [27] proposes a novel application of neural network in evaluating multiple recommendations of various trust standards. This contribution presents the design of a trust model to derive recommendation trust from heterogeneous agents. The experimental results show that the model has robust performance when there is high prediction accuracy requirement or when there are deceptive recommendations.

Moreover, other trustworthiness models were proposed without neuronal networks methods [28, 29], such as similarity approaches. In [29], it is stated that predicting trust among the agents is of great importance to various open distributed settings. The author focus the study on peer-to-peer systems in that dishonest agents can easily join the system and achieve their goals by circumventing agreed rules, or gaining unfair advantages. These cases are closely related to e-assessment regarding anomalous assessment processes as well as integrity and identity security properties. To this end, this work proposed a trust prediction approach to capture dynamic behaviour of the target agent by identifying features, which are capable of describing context of a transaction. A further work [28], on users' ratings systems, presents experimental results which demonstrate that ratings volume is positively associated with trust, as well as the congruence between one's own and others' opinions. This study also demonstrates that ratings source and volume interact to impact credibility perceptions, reliance on user-generated information, and opinion congruence. These results indicate important theoretical extensions by demonstrating that social information may be filtered through signals indicating its veracity, which may not apply equally to all social users.

2.7. Previous Trustworthiness Methodological Approaches

To date, little research has been carried out to build trustworthiness methodological approaches. However, in the context of business processes, the authors in [30], propose a generic methodology, called Trustworthiness Measurement Methodology (TMM). This methodology can be used to determine both the quality of service of a given provider and the quality of product. The scope of this study are the business processes, but the key concept of this methodology is the interaction between agents. Indeed, this is the same topic that we study in collaborative learning, but in our context, considering students' interactions and trustworthiness between them. This methodology is based on the following phases:

1. Determine the context of interaction between the trusting agent and the trusted entity.
2. Determine the criteria involved in the interaction.
3. Develop a criterion assessment policy for each criterion involved in the interaction.
4. Determine the trustworthiness value of the trusted entity in the given context.

In [31], the authors presented the foundations of formal models for trust in global information security environments, with the aim of underpinning the use of trustworthiness based security mechanisms as an alternative to the traditional ones. As stated by the authors, this formal model is based on a novel notion of trust structures, which is built on concepts from trust management and domain theory as well as features at the same time a trust and an information partial order. The formal model is focused on the following target aspects:

1. Trustworthiness involves entities.
2. Trustworthiness has a degree.
3. Trustworthiness is based on observations.
4. Trustworthiness determines the interaction among entities.

In addition to the methodology and formal approaches, in another work [32], a trust architecture is presented by introducing a basic trust management model.

3. Trustworthiness and Security Methodology Approach

In this section, we first describe the main theoretical features of our methodological approach and then, the summary of its key phases is presented. Finally, we detail each phase by analysing the processes, data, and components involved in the methodology.

3.1. Theoretical Analysis

In these sections, we present our methodological approach called Trustworthiness and Security Methodology (TSM) in CSCL. TSM is a theoretical approach devoted to offering a guideline for designing and managing security in mobile collaborative e-Learning activities through trustworthiness assessment and prediction.

TSM is defined in terms of TSM cycles and phases, as well as, components, trustworthiness data and main processes involved in data management and design. We define a TSM phase as a set of processes, components, and data. TSM phases are sequentially arranged and the three main phases (see Fig. 1) in TSM form a TSM design and deploy cycle (i.e. TSM-cycle). Each TSM-cycle corresponds to an interaction over the overall design process. Firstly, these concepts are presented as a methodological approach and then we complete the theoretical analysis with those methods and evaluation processes that we discussed in our previous research [11, 12, 13].

TSM aims to deliver solutions for e-Learning designers. TSM supports all analysis, design, and management activities in the context of trustworthiness collaborative learning activities, reaching security levels defined as a part of the methodology. Therefore, TSM tackles the problem of security in CSCL through the following guidelines and main goals:

1. Define security properties and services required by e-Learning designers.
2. Build secure CSCL activities and to design them in terms of trustworthiness.
3. Manage trustworthiness in learning systems with the aim of modelling, predicting, and processing trustworthiness levels.

4. Detect security events which can be defined as a condition that can violate a security property, thus introducing a security breach in the learning system.

The scope of our methodological approach is an e-Learning system formed by collaborative activities developed in a Learning Management System (LMS). The LMS has to provide support to carry out these activities and to collect trustworthiness data generated by learning and collaboration processes. Although in the context of collaborative e-Learning we can consider several actors with different roles in the overall process, for the sake of simplicity, we only consider the most significant actors and roles related to this research, as follows:

1. Students, as the main actors in the collaborative learning process and as targets of the trustworthiness analysis.
2. Designers, that represent the role in charge of all e-Learning analysis and design tasks.
3. Managers, that develop management processes, such as deployment, monitoring or control tasks.

3.2. Methodology Key Phases

As shown in Fig. 1, the TSM methodology is divided into three sequential phases:

1. Building Trustworthiness Components, integrated into the design of secure collaborative learning activities.
2. Trustworthiness Analysis and Data Processing, based on trustworthiness modelling.
3. Trustworthiness Assessment and Prediction, to detect security events and to refine the design process.

Although we assess each phase of the methodology as potential sets of concurrent processes (see next sections), these core phases have to be developed following the sequential phases presented. The main reason for defining this sequential model is the input and output flow. In other words, the output of one phase is the input of the next one. For instance, we can only start the data collection phase when trustworthiness components are deployed. Likewise, we cannot start trustworthiness prediction or assessment until data processing has been completed.

Despite the sequential model between each phase, we can consider the overall process, formed by these three phase, as a TSM-cycle. Each TSM-cycle allows e-Learning designers to improve the collaborative learning activities from the results, and trustworthiness decision information retrieved from the previous cycle. This information can introduce design enhances which will be deployed in the next deployment (i.e. the next time that the students will carry out the activity supported by the learning component). In terms of the data flow between TSM-cycles, the input for the new design iteration is the trustworthiness decision information. For instance, if decision information shows that there exist a deficiency in a component, the detected impediment can be overcome through design changes that are deployed in the next TSM-cycle execution.

3.3. Building Trustworthiness Components

The first phase of TSM deals with the design of collaborative activities. The key challenge of the design process is to integrate trustworthiness data collection inside the learning process. In other words, the trustworthiness component has to carry out its learning purpose. In addition, the learning component has to produce trustworthiness basic data. Moreover, data collection methods and processes should not disturb the learning activity. To this end, we propose the processes, data, and components that can be seen from the diagram in Fig. 2. Due to the first goal of the methodology is to design the trustworthiness component, we divide this phase into the following analysis considerations:

1. Collaborative learning activities generate a significant amount of interactions. Due to students' interactions are closely related to trustworthiness modelling, designers have to consider and analyse each interaction, which may be related to trustworthiness.
2. Analyse and determine relations between students' interaction and trustworthiness could be a challenging task in e-Learning design. Hence, we propose the study of trustworthiness factors [11], which can be defined as those behaviours that reduce or build trustworthiness in a collaborative group. Trustworthiness factors can be divided into trustworthiness reducing factors and trustworthiness building factors. This resource will allow designers to determine those interactions, which may generate trustworthiness basic data.
3. Designers have to model security issues so that they are compatible with trustworthiness data and students' interactions.

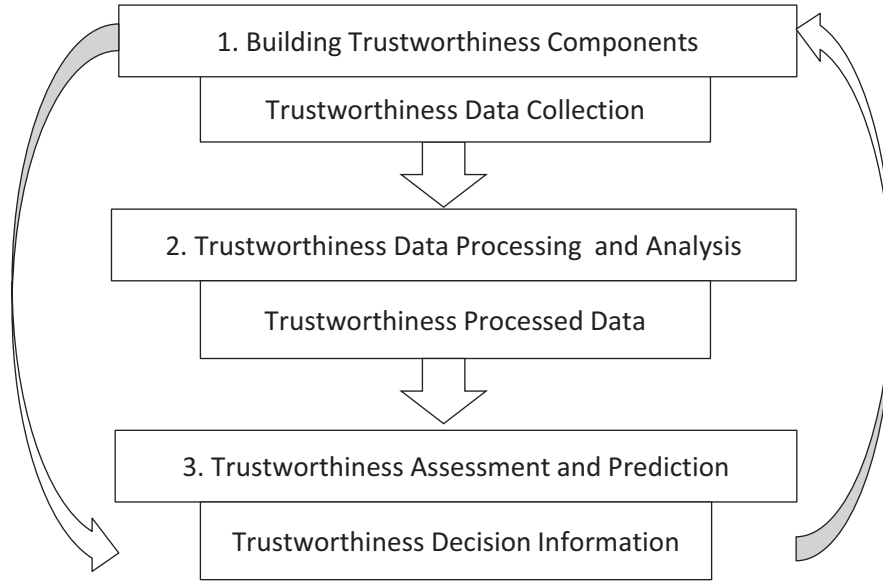


Figure 1: TSM Key Phases

Based on the above considerations, we propose the analysis of general security properties and services presented in [4]. Through selecting and analysing security properties we can connect trustworthiness, interactions, and security requirements in terms of collaborative learning activities.

From the study of security properties, students' interactions and trustworthiness factors, the initial collaborative learning activity has evolved to a peer-to-peer assessment component. Once we endowed the collaborative activity with security and trustworthiness, the next process is focused on data collection. To this end, we define research instruments for data collection intended to retrieve all trustworthiness data generated by the peer-to-peer assessment component.

Note that, for the sake of simplicity, we present a case dealing with one collaborative activity only, which generate its peer-to-peer assessment component. Despite this, the case may be extended to a set of collaborative activities implemented in one or several peer-to-peer components. Moreover, the components can be supported by several research instruments or a peer-to-peer component, including multiple collaborative activities. Eventually, the result in any case (i.e. single and multiple activities, components and instruments) is a set of trustworthiness basic data that will feed the next phase of the methodology. For this reason, we define the input of the next phase in terms of multiple trustworthiness data sources.

We suggested the need of modelling activities, components, security properties, or interactions in the context of a general design process. This process may be a challenge if the e-Learning designer does not use suitable modelling tools. To overcome this impediment, we reviewed the Educational Modelling Language (EML) [33] that, with the indications presented in [4], allows designers to tackle with modelling security, CSCL activities and interactions.

3.4. Trustworthiness Analysis and Data Processing

So far, the e-Learning designer has built the trustworthiness component, which will be deployed in the LMS. It is worth mentioning that the deployment of collaborative learning activities may involve multiple LMSs. In fact, we are proposing a learning activity deployment in conjunction with research instruments for data collection. The implementation of these instruments may require additional technological solutions such as normalization processes. Trustworthiness modelling and normalization processes in TSM (see Fig. 3) are based on the key concepts presented in the rest of this subsection (further information and details of these concepts can be found in our previous research [11, 12, 13]).

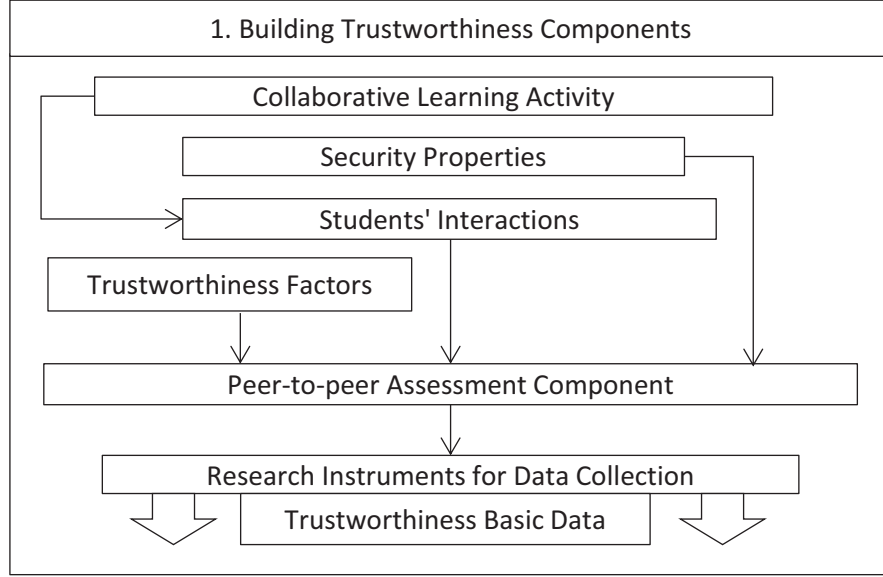


Figure 2: Phase 1: Building Trustworthiness Components

We introduced the concept of Trustworthiness Indicator as a measure of trustworthiness factors. Trustworthiness factors were presented (see Section 3.3) as those behaviours that reduce or build trustworthiness in a collaborative activity and they were integrated in the design of research instruments. Therefore, we define a Trustworthiness Indicator as a basic measure of a trustworthiness factor that is implemented by a research instrument and integrated in the peer-to-peer assessment component. Finally, Trustworthiness Levels can be defined as a composition of trustworthiness indicators. The concept of levels is needed because trustworthiness rules and characteristics must be considered and, consequently, we have to compose this more complex measure [11].

Regarding normalization functions there are several reasons that impede the management and processing of trustworthiness levels directly. Among them, we can highlight several aspects, such as multiple sources, different data formats, measure techniques and other trustworthiness factors such as rules, trustworthiness evolution, or context. Therefore, both trustworthiness indicators and levels have to be normalized through normalization functions. The selection of these functions depend on the data sources and the format selected for each instrument for data collection [13].

Once trustworthiness modelling concepts are defined, the task of data processing starts, and then basic data from trustworthiness data sources is computed in order to determine indicators or levels, for each student, group of students, evaluation components, etc. The main challenge of data processing in this case is that extracting and structuring these data is a prerequisite for trustworthiness data processing. In addition, with regarding to computational complexity, extracting and structuring trustworthiness data is a costly process. Moreover, the amount of basic data tends to be very large [12]. Therefore, techniques to speed and scale up the structuring and processing of trustworthiness basic data are required (see [12] for a parallel implementation approach to be developed in the context of trustworthiness data processing).

3.5. Trustworthiness Assessment and Prediction

From the trustworthiness data computed in the previous phase, we can carry out both assessment and prediction processes, which allow e-Learning managers to make security decisions based on the output of this phase (i.e. trustworthiness decision information). Furthermore, this information can be taken into account as input data for an iterative design process as mentioned in Section 3.2.

Trustworthiness assessment and prediction stems from the analysis of the time factor in trustworthiness. Fig. 4 shows how trustworthiness assessment and prediction begins with the conversion of processed data into trustwor-

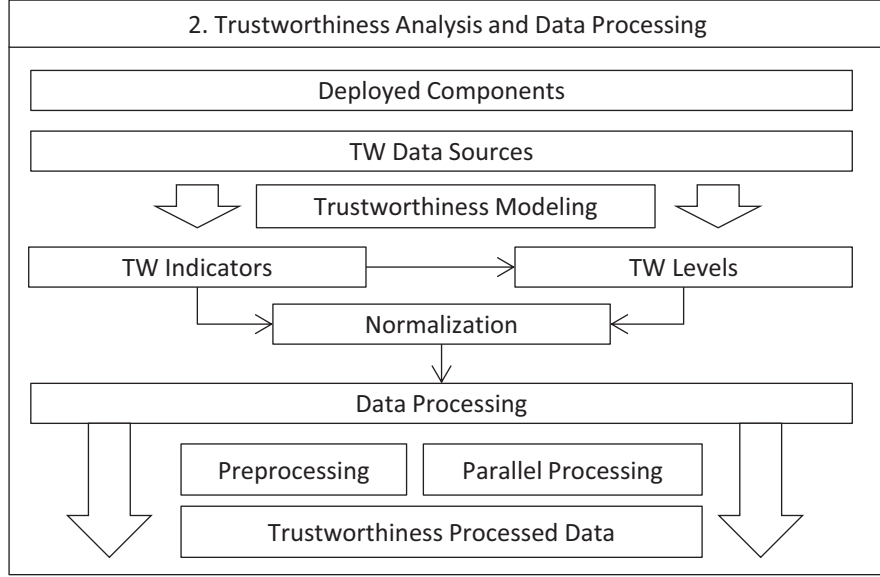


Figure 3: Phase 2: Trustworthiness Analysis and Data Processing

thiness sequences by considering the time factor. The concept of trustworthiness sequence is related to levels and indicators and can be defined as the ordered list of a student's trustworthiness normalized levels when the student is performing the peer-to-peer assessment component over several points in time.

Once trustworthiness sequences are built, the e-Learning manager is able to set out predictions and assessment processes. As presented in [11], methods intended to predict and assess trustworthiness are available in the context of peer-to-peer assessment. The e-Learning designer has to select and determine suitable methods for the specific target scenario.

We cannot use trustworthiness decision information (i.e. reliable trustworthiness information) without the validation process. The validation process is intended to filter anomalous cases, to compare results that represent the same information from different sources, and to verify results using methods such as similarity coefficients. Nevertheless, this information may indicate signs and the complex nature of trustworthiness modelling requires additional validation processes. These validation models can be classified into internal and external, and each type may involve automatic and manual tasks. For instance, in the context of e-assessment, we could compare trustworthiness results generated by the peer-to-peer assessment component to external (respect to the peer-to-peer component) results from the manual tutor evaluation. Moreover, this comparison could be automatically developed by the system and analysed by the tutor before taking any decision.

Finally, trustworthiness decision information is available and then e-Learning managers can analyse valid and useful information devoted to reporting security events, improve the framework design, or manage security enhances. In the rest of the paper we present specific TSM aspects in real online courses, focused on trustworthiness assessment (see Section 4) and trustworthiness prediction (see Section 5).

4. Trustworthiness Methodology Evaluation

In order to evaluate and support the application and deployment of TSM, in this section, we concrete several significant aspects of TSM. These aspects are considered in terms of specific methods and techniques through their application in real online courses.

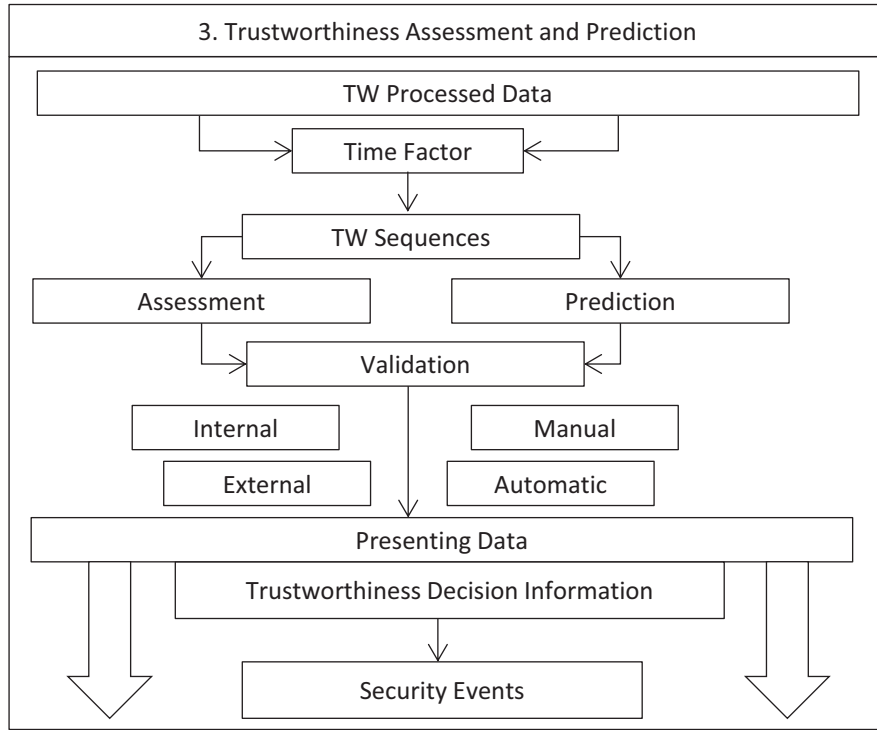


Figure 4: Phase 3: Trustworthiness Assessment and Prediction

4.1. Real Online Courses

We carried out two studies [12, 34] based on real online courses at the Open University of Catalonia¹. These studies were performed with the aim to experiment with specific trustworthiness methods and techniques involved in TSM as well as to illustrate specific applications and to evaluate the feasibility of the TSM.

In the first study [12], the mobile collaborative activities represented a relevant component of the e-assessment of the course. Students' evaluation was based on a hybrid continuous evaluation model by using several manual and automatic evaluation instruments. There were 12 students distributed in three groups and the course was arranged in four stages. These stages were taken as time references in order to implement trustworthiness sequences. At the end of each collaborative stage, each student had to complete a survey. The coordinator of the group had to complete two reports, public and private, and at the end of each stage, the members the group was evaluated by the coordinator. General e-Learning activities were supported by a standard LMS, which offered both rating systems and general learning management indicators. Given the low number of students, we could study the data in much more detail and flexibility. Likewise, we could experiment with several design alternatives and adapting the model to the design cycles proposed in TSM (see Section 3).

The second study [34] extended the scope of the first one to a more standard scenario in which we could not manage so much flexibility and manual processes. The course was focused on peer-to-peer e-assessment and it has the following main features:

- Students' assessment was based on a continuous assessment model by using several manual assessment instruments. Manual assessment was completed with automatic methods, which represented up to 20 percent of the total student's grade. Therefore, we implemented a hybrid assessment method, which combined manual and automatics assessment methods, and the model allowed us to compare results in both models.

¹<http://www.uoc.edu>

- Number of students participating: 12 students performed a subjective peer-to-peer assessment, that is, each student could assess any student in the classroom following the assessment design.
- The course followed seven stages that could be taken as time references in order to validate and to analyse results. Each stage corresponded to a module of the course, which had a learning module (i.e. book) that the student must study before developing the assessment activities of the course.

From the above base course features, we built the peer-to-peer e-assessment activity encapsulated as a Continuous Assessment (CA), which was formed by three assessment activities (described in the rest of this section). Once the student has studied a module, the student receives an invitation to answer (i.e. a short text response) a set of evaluation questions about the current module. This is the first activity of the CA named the Module Questionnaire and denoted by Q. The student did not have to answer as soon as Q was sent, because the second activity of the CA was a students' forum (F) intended to create a mobile collaborative framework devoted to enhancing responses in activity Q, in other words, Q and F activities are concurrent tasks. The final activity was the core of the peer-to-peer assessment and the student has to complete a survey (P) which contained the set of responses from Q. The student had to assess each classmate's responses in Q and, furthermore, the activity of each student in the forum F was assessed. These collaborative activities were designed considering the use of mobile devices.

4.2. Building Collaborative Components with TSM

After the experience designing components in the first study, in the second one, we built a comprehensive peer-to-peer assessment component. We selected integrity and identity as target security properties for the component and, after the analysis of potential students' interactions in basic activities, the first version of the peer-to-peer assessment component was proposed.

The final version of the component had three stages: Once the student had studied a module, the student received an invitation to a survey (S1) with questions about the current module. Students did not have to answer S1 as soon as the invitation was received. The second activity of the component was a students' forum (F), which created a collaborative framework devoted to enhancing responses' quality in S1. Eventually, the student had to complete another survey (S2), which contained the set of responses over the first one (S1). By using S2, the student had to evaluate each classmate's responses as well as the participation of each student in the forum F. The design of this activity endorsed our proposal regarding the analysis of security properties, students' interactions, and factors.

Regarding research instruments and data collection, we included the following instruments:

1. Surveys.
2. Ratings.
3. Students reports.
4. LMS indicators.

To sum up, each instrument was integrated into the mobile collaborative activity (through mobile tools) and it managed its own data formats.

4.3. Notation and Terminology in TSM

Before the analysis and data processing phase, we introduce the key terms presented in the next sections (see Table 1).

4.4. Analysis and Data Processing with TSM

We analysed research instruments data formats in terms of data sources in TSM. For each case, we selected a set of normalization functions intended to convert basic trustworthiness data in normalized trustworthiness values. Normalization functions are combined with trustworthiness levels and indicators. As an example of this combination, when a student evaluates every classmate's responses, we use the following normalization function [13]:

$$N\left(tw_{R_{q,m,s}}\right) = \sum_{j=1}^{N_S} \frac{tw_{R_{q,m,j}}}{N_S - 1}, j \neq s, N_S = |S|, q \in Q, m \in M, s \in S, j \in S \quad (1)$$

Table 1: Notation and Terminology

tw_i	A trustworthiness indicator tw_i as a measure of trustworthiness factors.
$i \in I$	The set of trustworthiness indicators.
N_I	The number of trustworthiness indicators.
$m \in M$	A module m in the set of modules M .
N_M	The number of modules.
$q \in Q$	A question q in the set of questions Q .
N_Q	The number of questions.
$s \in S$	A student s in the set of students S .
N_S	The number of students.
DS_{ca}	The Continuous Assessment (CA) Data Sources, $ca \in \{R, F, Q_r, Q_c\}$.
DS_{Q_r}	The questionnaire DS for the students' responses.
DS_{Q_c}	The questionnaire DS for the number of responses.
DS_R	The peer-to-peer questionnaire DS for the score that a student has assessed a student's response.
DS_F	The forum participation DS for the number of posts.
$N()$	Normalization function to convert basic indicators in normalized trustworthiness values.
w_i	The component normalization weight for the indicator tw_i , $w_i \in (w_1, \dots, w_n)$.
$N_2()$	Normalization function for responses data source DS_R .
$N_4()$	Normalization function for forum participation data source DS_F .
$tw_{caq,m,s}$	Trustworthiness indicator for the Continuous Assessment (CA) component.
$tw_{caq,m,s}^N$	Normalized trustworthiness indicator for the CA component.
$tw_{Rq,m,s}$	The trustworthiness indicator for the students' responses score data source DS_R .
$tw_{F,m,s}$	The trustworthiness indicator for the forum participation.
L_I^N	The generic normalized trustworthiness level.
$L_{R,m,s}^N$	The normalized trustworthiness level for students' responses.
$L_{F,m,s}^N$	The normalized trustworthiness level for forum participation.
$L_{m,s}^N$	The overall normalized trustworthiness level.
$CATS_s$	The Continuous Assessment Trustworthiness Sequence (CATS) ordered list.
$CATS$	The CATS matrix.
$CATS_s^a$	The active CA trustworthiness history sequence.
$CATS_s^c$	The constrictive trustworthiness history.
$CATS_s^W$	The trustworthiness window sequence.

where $tw_{Rq,m,s}$ is the responses (R) indicator, s is the target student (i.e. the student evaluated), N_S is the number of students in the course, and q is the one of the questions evaluated in the module m .

With respect to trustworthiness normalized levels Ltw^N , we managed several indicators composition. The most suitable level in both courses is based on a weight model:

$$Ltw^N = \sum_{i=1}^{N_I} \frac{tw_i \cdot w_i}{N_I}, i \in I, w_i \in (w_1, \dots, w_{N_I}), \sum_{i=1}^{N_I} w_i = 1, N_I = |I| \quad (2)$$

where N_I is the total number of trustworthiness indicators and w_i is the weight for the normalized indicator tw_i .

Regarding data processing, we experimented with sequential and parallel implementations [12]. Sequential approaches were feasible to manage data sources from several activities, such as responses in a survey or number of posts in a forum. However, processing the log data took too long to complete and it had to be done offline (i.e. after the completion of the learning activity). For this reason, we endowed our trustworthiness framework with parallel processing facilities.

To this end, we designed a MapReduce algorithm [12] implemented in an Apache Hadoop² and deployed in the

²<http://hadoop.apache.org>

RDlab³ computing cluster. Using this model, a considerable speed up was achieved in processing large log file, namely, more than 75% for 10 nodes (see [12] for the whole results).

4.5. Assessment, Prediction and Evaluation with TSM

Peer-to-peer components were designed considering the time factor. Activities are arranged in stages that conduct the definition of trustworthiness sequences. In both studies, trustworthiness indicators and levels are instanced in points of time (e.g. the same indicator measured for each module) and arranged in trustworthiness sequences. The concept of trustworthiness sequence in an evaluation component allows us to support assessment and prediction. Actually, it could be directly incorporated, in some cases, as input for assessment and prediction methods. Regarding validation, we experimented with a hybrid validation approach by combining manual, automatic, external, and internal validation methods. As an example of this model, we analysed similarity between manual evaluation results and automatic trustworthiness levels. The method to tackle similarity proposed is based on Pearson correlation [35].

Finally, we consider two different methods to deal with prediction. The first approach is based on neural networks [21] and the second one on collaborative filtering. On the one hand, a neural network captures any type of non-linear relationship between input and output. In our case, the input is the trustworthiness history sequence and the output is the prediction calculated by the neural network (i.e. trustworthiness predicted value). On the other hand, filtering recommendation algorithms concern the prediction of the target user's assessment, for the target item that the user has not given the rating, based on the users' ratings on observed items. In our context, items involved in the recommendation system are the students themselves.

In the rest of this paper, we focus the validation of TSM on trustworthiness prediction based on a neuronal network approach. Furthermore, the methods presented in this section (i.e. trustworthiness data sources, indicators, normalizations processes, and history sequences) are also applied from the view of trustworthiness prediction.

5. Evaluation of Trustworthiness Prediction

In this section, a trustworthiness prediction model is presented in the context of the real online course based on peer-to-peer e-assessment described in Section 4.1.

5.1. Normalizing Trustworthiness Data Sources

Once the peer-to-peer e-assessment has been designed, we analyse and define trustworthiness data sources and levels. In the context of Continuous Assessment (CA), we defined a trustworthiness data source as those data generated by the CA that we use to define trustworthiness levels as presented in [11, 12, 13]. Each CA correspond to a module $m \in M$, which is a unit of the course. The modules will be used as a point in time references. Each CA (i.e. one CA per module) will manage three data sources, which are denoted with the following ordered tuples:

$$DS_{Q_C} = (M, Q, S, count) \quad (3)$$

where the questionnaire data source DS_{Q_C} is defined as the total number of responses (*count*) that each student in S has answered in the questionnaire Q for the module M .

$$DS_{Q_R} = (M, Q, S, res) \quad (4)$$

where the questionnaire data source DS_{Q_R} is defined as the response *res* (i.e. a student answers *res* to a question) that each student in S has responded regarding a specific question in Q in the module M .

$$DS_F = (M, F, S, count) \quad (5)$$

where the forum participation data source DS_F is defined as the total number of posts (*count*) that each student in S sent to a forum F regarding a specific question in Q in the module M .

³<http://rdlab.lsi.upc.edu>

$$DS_R = (M, Q, S, SS, score) \quad (6)$$

where the responses data source denotes the score that a student (in S) has assessed a student's (in SS) response of a question in Q . Hence, S is the set of students who assess and SS is the set of students who are assessed by students in S .

In this case, modelling trustworthiness involves multiple complex and heterogeneous data sources with different formatting, which cannot be managed without normalization. According to the model presented in [13], we define a normalized trustworthiness indicator for the case of an CA as follow:

$$tw_{ca_{q,m,s}}^N = N \left(tw_{ca_{q,m,s}} \right), ca \in DS_{R,F,Q_r,Q_c}, q \in Q, m \in M, s \in S \quad (7)$$

where DS_{R,F,Q_r,Q_c} are the CA data sources, S is the set of students, M is the set of modules, and Q is the set of questions in each module.

We now define the normalization functions. Note that although in [13] we included four normalization functions, in this case, a subset is selected: N_2 and N_4 . The reason for this is that we focus the data analysis on two data sources, forum participation (N_4) and questionnaires (N_2). Regarding the responses data source R , a student can assess every classmate's responses. To this end, we use the normalization function N_2 :

$$N_2 \left(tw_{R_{q,m,s}} \right) = \sum_{i=1}^{N_S} \frac{tw_{R_{q,m,i}}}{N_S - 1}, i \neq s \quad (8)$$

where $tw_{R_{q,m,s}}$ is the responses indicator, s is the target student (i.e. the student who is assessed), N_S is the number of students in the course, and q is the one of the questions assessed in the module m .

It is worth mentioning that the scale for $tw_{R_{q,m,s}}$ must be converted to integer values before normalizing with function N_2 . Similarity, the forum participation indicator also needs normalization. In this case, we apply the normalization function N_4 :

$$N_4 \left(tw_{F,m,s} \right) = \frac{tw_{F,m,s}}{T_F}, m \in M, s \in S \quad (9)$$

where T_F is the maximum number of post in the forum by an student s in the module m .

5.2. Trustworthiness Levels and Sequences in e-Assessment

We normalize the trustworthiness indicators for forum participation and responses (i.e. a student answers a question in the questionnaire). Then, trustworthiness levels [11] are defined in order to measure students' overall trustworthiness. To this end, we define the following trustworthiness levels:

$$L_I^N = \sum_{i=1}^{N_I} \frac{(tw_i^N * w_i)}{N_I}, i \in I, w_i \in (w_1, \dots, w_{N_I}), \sum_{i=1}^{N_I} w_i = 1 \quad (10)$$

where N_I is the total number of trustworthiness indicators and w_i is the weight assigned to tw_i .

Following this model, we first combine the trustworthiness indicators of each question in the module and then, the overall trustworthiness level for the student in a specific module $m \in M$ is defined:

$$L_{R,m,s}^N = \sum_{q=1}^{N_Q} \frac{(tw_q^N * w_q)}{N_Q}, q \in Q, N_Q = |Q|, \sum_{q=1}^{N_Q} w_q = 1, w_q = \frac{1}{N_Q}, m \in M, s \in S \quad (11)$$

$$L_{F,m,s}^N = N_4(tw_{F,m,s}), m \in M, s \in S \quad (12)$$

$$L_{m,s}^N = \sum_{j=1}^2 \frac{(Ltw_j^N * w_j)}{2}, j \in \{L_{F,m}^N, L_{R,m}^N\}, \sum_{j=1}^2 w_j = 1, w = (0.4, 0.6), m \in M, s \in S \quad (13)$$

where $L_{m,s}^N$ is the overall trustworthiness level for the student s in the module m , calculated by combining the trustworthiness level for responses $L_{R,m,s}^N$ and the trustworthiness level for forum participation $L_{F,m,s}^N$.

Once trustworthiness levels are defined, we endow our model with time factor. Although the concept of trustworthiness sequence was defined in the context of grid services and requesters [25], it is feasible to apply this approach to another modelling scenario such as peer-to-peer e-assessment. The only requirement is time factor, in other words, the model should allow us to compute an overall trustworthiness level referred to multiple points of time. Therefore, we define Continuous Assessment Trustworthiness Sequence CATS as the ordered list of a student's trustworthiness history levels over several points in time:

$$CATS_s = (L_{m_1,s}^N, \dots, L_{m_k,s}^N, \dots, L_{m_{N_M},s}^N) m_k \in M, s \in S \quad (14)$$

where M is the set of modules, each module m_k refers to a point in time and $L_{m_k,s}^N$ is the overall trustworthiness level for the student s in the module m_k .

Likewise, we can define the overall students' CA trustworthiness history sequence as the matrix:

$$CATS = \begin{pmatrix} L_{m_1,s_1}^N & \dots & L_{m_1,s_{N_S}}^N \\ \vdots & \ddots & \vdots \\ L_{m_{N_M},s_1}^N & \dots & L_{m_{N_M},s_{N_S}}^N \end{pmatrix} \quad (15)$$

where N_M is the number of modules (i.e. points in time analysed), and N_S is the number of students in the course.

5.3. Trustworthiness Sequences Results

Processing trustworthiness sequences results involves large amount of data generated by the peer-to-peer activity of the CA. To this end, we compute the following elements:

1. The trustworthiness history sequence matrix has $N_S * N_M$, $N_S = |S|$, $N_M = |M|$ elements.
2. For each element in $CATS$, $L_{m,s}^N$, we compute both forum participation and responses trustworthiness levels.
3. Although forum participation is a single indicator, with respect to responses, there are three different questions.
4. Moreover, for each trustworthiness levels we compute each student's score for the indicator.

With the aim of managing this trustworthiness sequences results, we developed a data parse *Java* tool called *parse_tw_tuples* that converts peer-to-peer values into basic tuples presented above. This tool generates basic tuples from the web applications and these primitive records can be imported in a relational database for further processing. In order to deal with the results, we have to consider the size of the result set of records generated by each data source. At the end of the process the responses data source maximum size is:

$$|DS_R| = |M| \times (|Q| + 1) \times |S| \times |S| \quad (16)$$

where $|M|$ is the number of modules, $|Q|$ is the number of questions (+1 is added because the student also assesses the forum activity), and $|S|$ is the number of students who could participate in both questionnaires (i.e. Q and P).

The total number of computed tuples is:

$$|DS_R| = 10.522 \quad (17)$$

To sum up, the diagram depicted in Fig. 5 shows the overall process including how we have to normalize data sources. Then, this figure shows the creation of trustworthiness indicators and levels, and finally, the procedure presented to compose trustworthiness sequences.

5.4. Predicting with Trustworthiness Sequences

So far, we have presented the design of trustworthiness history sequences in the peer-to-peer assessment components of the target online course. To this end, we have to consider the main concepts presented in [25] related to trustworthiness history sequence as a foremost step in trustworthiness prediction based on neural network design.

Active trustworthiness history sequence is the recent trustworthy history sequence. Then, we define active CA trustworthiness history sequence $CATS_s^a$ as the ordered list of students' trustworthiness levels over the points in time:

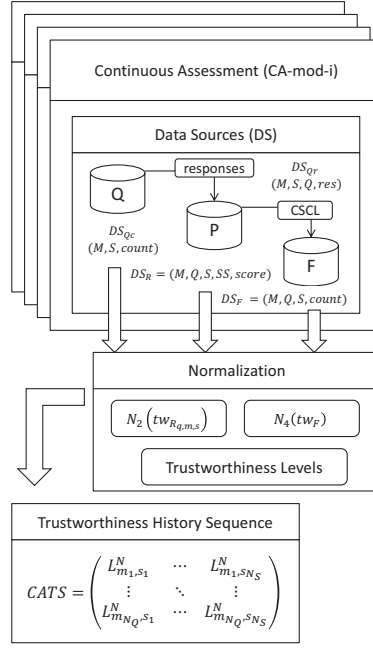


Figure 5: CA data sources, normalization and trustworthiness sequences

$$CATS_s = (L_{m_1,s}^N, \dots, L_{m_k,s}^N, \dots, L_{m_{N_M},s}^N), m_k \in M, s \in S \quad (18)$$

$$CATS_s^a = (L_{m_{NQ-a+1},s}^N, L_{m_{NQ-a+2},s}^N, \dots, L_{m_{N_M},s}^N), s \in S \quad (19)$$

where M is the set of modules, each module m_k refers to a point in time, and $L_{m_k,s}^N$ is the overall trustworthiness level for the student s in each module.

Constrictive trustworthy history is the subsection average of active trustworthy history sequence.

$$CATS_s^c = (L_{m_1 \dots N_S,s}^N, L_{m_{r+1} \dots N_Q,s}^N, \dots), s \in S \quad (20)$$

where each element in the tuple is the average of a subset of elements in $CATS_s^a$, and k is the number of inputs of NN.

These tuples are presented in order to prepare those input sets that are required in neural network training and validation. The concept of trustworthiness sequences in prediction with neural networks is also suggested in [21]. In this proposal, the trustworthiness sequence is split into subsequences of fixed sizes, without average transformation:

$$CATS_s^w = (L_{m_1,s}^N, \dots, L_{m_w,s}^N), (L_{m_{w+1},s}^N, \dots, L_{m_{2w},s}^N), \dots, s \in S \quad (21)$$

where each component in the trustworthiness window is a subset of the $CATS_s$.

5.5. Designing a Neural Network e-Assessment Proposal

We reviewed complementary related trustworthiness prediction work. Among existing models, we select the neural network-based approaches for predicting trust values presented in [21] and [25], because these approaches are feasible in the context of e-assessment. These models present several significant differences, especially with respect to how to build training sets, these differences are considered in our e-assessment proposal. Although we evaluated both approaches, in the rest of the paper, we address our NN design to a training model based on $CATS_s^w$. We consider this approach more suitable for our case because $CATS_s^w$ generates a greater amount of training sequences.

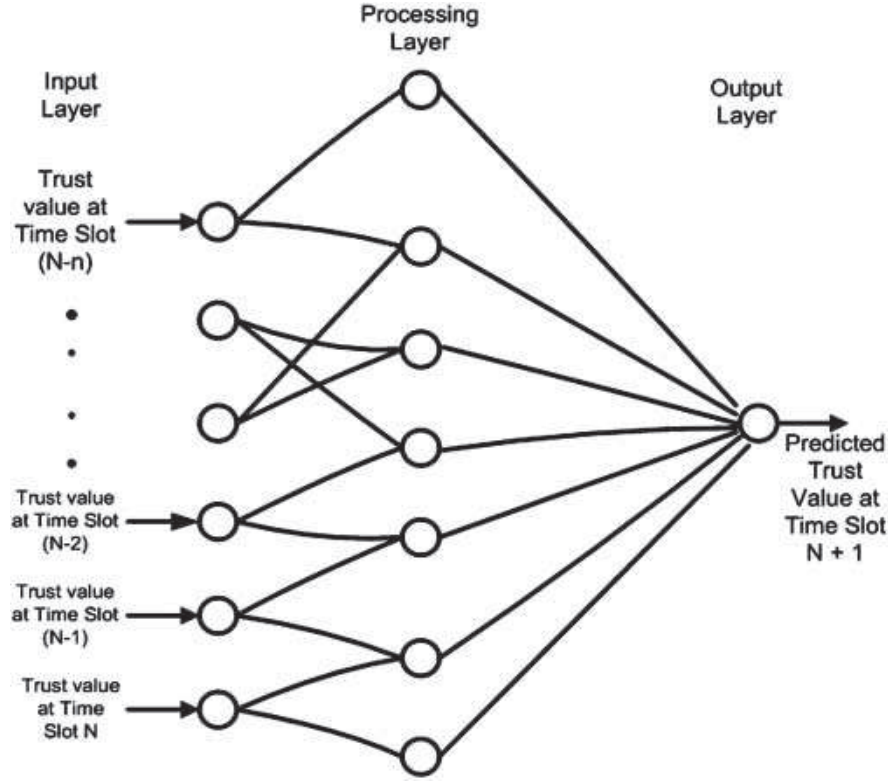


Figure 6: A simple NN approach for trust prediction [21]

A neural network can capture any type of non-linear relationship between input and output data through iterative training. In our case, the input is the CA trustworthiness history sequence formed by trustworthiness results generated by the peer-to-peer assessment component, and the output is the prediction calculated by the neural network (i.e. trustworthiness predicted value):

$$L_{m_{t+1},s}^N = NN(CATS_s), s \in S \quad (22)$$

where entity s denotes the student whose normalized trustworthiness level value is being predicted through the $CATS_s$ representing data generated by the peer-to-peer activity of the CA, and m_{t+1} denotes the trustworthiness point in time in the future predicted by the function NN for the student s (i.e. the output of the NN).

As presented in [21], the main principle of neural computing is the decomposition of the input-output relationship into a series of linearly separable steps using hidden layers. The NN architecture (see Fig. 6) is composed of sets of neurons that are arranged in multiple layers. The first layer, which inputs are fed to the network, is called the input layer. The last layer, which produces the NN output, is called the output layer. The layers in between these two layers (i.e. between input and output layers) are all hidden layers. The input consists of values that constitute the inputs for the hidden layers.

Every node computes a weighted function of its inputs and applies an activation function to compute the next output. The output is transmitted to all the connected nodes on the next layer with associated weights. The activation of each node depends on the bias of the node, which calculates the output as follows:

$$y_j = \sum_{i=0}^n w_{ij}x_i \quad (23)$$

where y is the result of the summation of the product of the input x with its associated interconnection weight w . The initial weights are assigned randomly but are gradually changed to reduce the error. The difference between the

desired output and the actual output constitutes the input to the back propagation algorithm for training the network based on the difference.

Through the iterative training, the NN produces better prediction accuracy in the domain of time series prediction, such as trustworthiness history sequences.

5.6. Simulation and Analysis of Results

With the aim of implementing the NN for trustworthiness prediction, we evaluated several simulators. Among them, we selected *Emergent*⁴ as a suitable software tool that reaches all the requirements for our case. Emergent (formerly PDP++) is defined as a comprehensive, full-featured deep neural network simulator that enables the creation and analysis of complex, sophisticated models [36]. The main reasons to use *Emergent* in the context of this paper can be summarized as follow:

- *Emergent* provides powerful visualization and infrastructure tools.
- Provides a structured environment for using and modify models based on NN templates, as well as, test and training programs.
- *Emergent* is completely open source software.
- Highly optimized runtime performance. In fact, we deployed the simulator environment in a virtual machine running on a personal computer.

With the aim of developing a first simulation approach in *Emergent*, we carried out the following tasks:

1. A new simulation project was created based on the template BpStd (i.e. standard initialization of back-propagation). This resource is provided by *Emergent* and allows the designer to begin the neuronal network design from a standard configuration.
2. As shown in Fig. 7 we generated and configured a standard network, specifying number of layers, layer names, sizes, types, and connectivity. The NN is formed by 3 layers with 2 input values and 1 output. In terms of *Emergent* design, a the geometry for both input and hidden layers is a 2 units x 1 units matrix.
3. The NN geometry corresponds to the size of the data contained in the *StdInputData* table. This table contains each student's each trustworthiness window sequence $CATS_s^W$ defined in Section 5.4. The data import process was managed through text file elements (see Fig. 8). *Emergent* offers import and export tools that bind the *StdInputData* tables and the text files.
4. Once NN basic design and input data were configured, the next step was the training process of the NN. Following the model defined in Section 5.4, we split the input values for each student into two trustworthiness sequences (i.e. training and test). The training trustworthiness window sequence contained 5 instances (i.e. time slots or modules in the course), which were arranged in tuples of 3 elements. The 3-tuple was also divided into the input values and the output result. Therefore, for each $CATS_s^W$ sequence we generate tuples of 3 elements containing the 2 input values and the output expected value.
5. The training process is managed by *Emergent* in the *BpTrain* program whose initial parameters are shown in Fig. 9.
6. Finally, we introduced the test elements in order to validate the model.

The deviation in prediction results for each student are depicted in Fig. 10. The sample of the experiment was formed by 12 students. Fig. 10 presents the results obtained from the NN simulation process for each students. The horizontal axis represents students and the vertical axis represents the difference between the value predicted by the NN and the test value (i.e. the prediction error in absolute value). For instance, the NN for the student 5 predicted a value with a 2,54% of error.

⁴<https://grey.colorado.edu/emergent/>

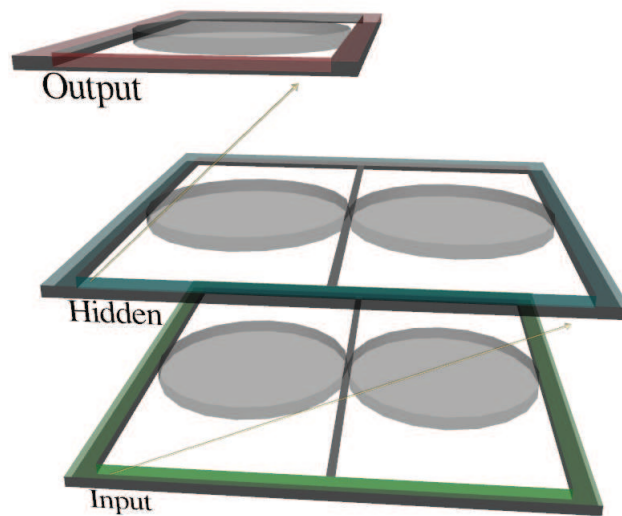


Figure 7: Standard network configuration with *Emergent*

The screenshot shows the Emergent software interface. The left sidebar displays a tree view of the project structure, including 'nn', 'docs', 'wizards', 'ctrl_panels', 'data', 'inputData', 'outputData', 'analysisData', 'programs', 'viewers', and 'networks'. The main window shows the 'ControlPanel' object, which contains a list of data items. The 'InputData' tab is selected, showing a list of data items with their types and values. The 'student-01.dat' file is open, displaying a table of data. The table has columns for 'Name', 'Input', and 'Output'. The data is organized into rows, with the first row being the header and the subsequent rows containing numerical values.

Name	Input	Output
0	1	(matrix)
1	2	(matrix)
2	3	(matrix)

Figure 8: Network *StdInputData* and text files

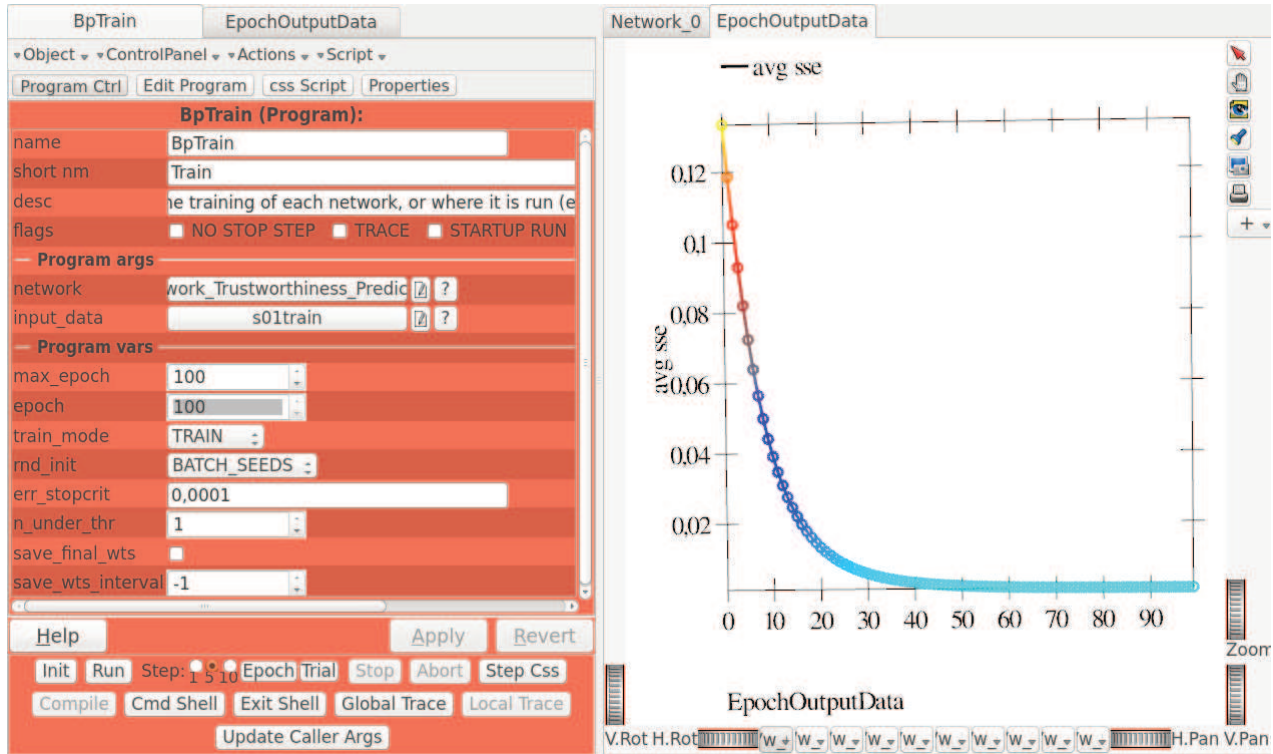


Figure 9: Training process parameters and simulation

Interestingly, regarding overall error prediction, the results reveal a notable similarity between the test and predicted values. However, the observed difference between the trustworthiness level through the modules is not significant. Therefore, the model is suitable for this students' trustworthiness behaviour, but we cannot demonstrate the stability of this prediction approach for other cases (i.e. more differences in trustworthiness evolution).

With respect to e-assessment security, the most significant finding is related to detect anomalous user assessment. From these data, 2 students (student 6 and 9), whose error prediction is greater than 3%, were found anomalous and required further investigation for potential cheating in order to validate the authenticity of the students' learning process.

Finally, we discovered that the number of modules in the course (i.e. the slots or the points in time) must be increased. If the number of training instances is increased, the student's NN will be able to accurately predict more trustworthiness different cases (not only those cases with low variation in trustworthiness evolution).

6. Conclusions and Further Work

In this paper, we first motivated the need to improve information security in mobile online collaborative learning and in particular MCSCL supported by mobile devices. To this end, we justified the feasibility of an approach focused on functional solutions, namely, based on trustworthiness assessment and prediction. The study reviewed the main works in the literature on security in mobile collaborative learning, how trustworthiness assessment and prediction is related to security, the time factor in trustworthiness modelling, and trustworthiness existing methodologies.

Then, we proposed an innovative trustworthiness and security methodological approach to build secure collaborative activities devoted to offering a comprehensive guideline for e-Learning designers and managers. The architecture of the methodology is based on building trustworthiness learning components, trustworthiness analysis and data processing, and trustworthiness assessment and prediction. We first described the main theoretical features of our methodological approach and then, the summary of its key phases is presented. Finally, we detailed each phase by analysing the processes, data, and components involved in the methodology.

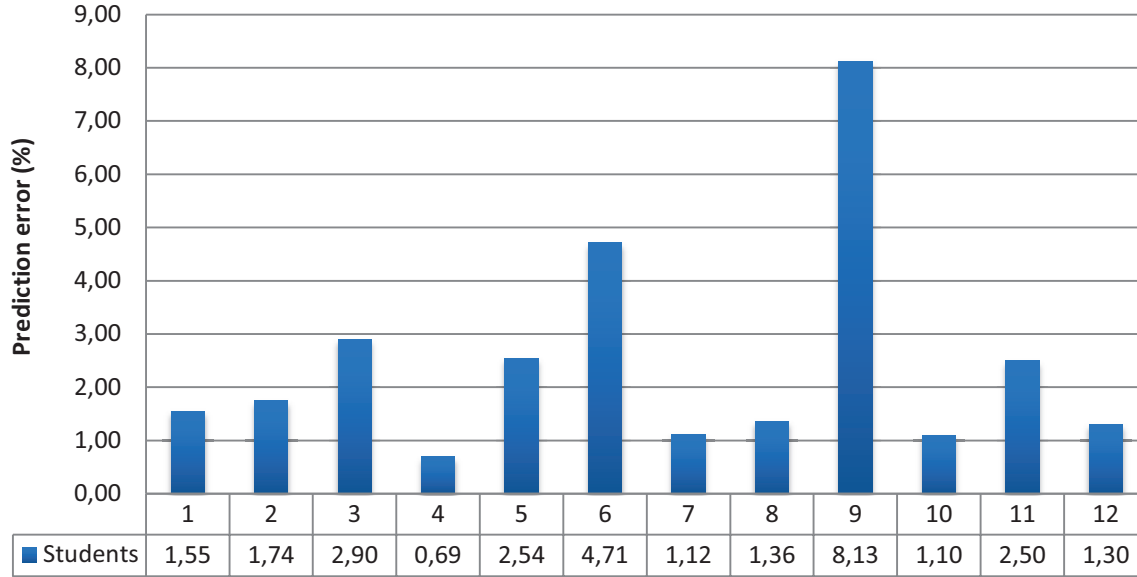


Figure 10: Students NN Prediction Results

The methodology was evaluated by presenting specific methods and techniques applied to real online courses. We used two studies, based on real online courses at the Open University of Catalonia, to evaluate and support the application and deployment of our trustworthiness methodology. Several significant aspects of our methodology were considered in terms of specific methods and techniques through their application in these real online courses.

Finally, we have presented an innovative prediction approach for trustworthiness behaviour to enhance security in online assessment. This study showed how neural network methods may support e-assessment prediction. These e-assessment prediction methods were performed in a real online course based on peer-to-peer assessment processes and mobile online collaborative activities. The processes and learning activities involved in the course, were encapsulated as continuous assessment component. Moreover, from this component, we presented the design of trustworthiness history sequences with the aim of designing a neural network e-assessment proposal.

The most relevant findings that emerge from the results presented in this paper, are related to trustworthiness methodological applications and trustworthiness prediction models. Regarding the trustworthiness methodology proposed, we supported the application and deployment of the methodology in two real online courses. The learning activities performed in the course were designed following the theoretical features, phases, data, and processes of our methodological approach. With respect to trustworthiness prediction, we demonstrated the feasibility of our neural network prediction approach. Regarding the overall error prediction, the results revealed a notable similarity between the test and predicted values. From these results, we were able to detect anomalous user assessment. From these data, 2 students, whose error prediction is greater than 3%, were found anomalous and required further investigation.

As ongoing work, we plan to continue the methodology testing and evaluation process by deploying its components in additional real online courses. Due to further deployments will require large amount of data analysis, we will continue investigating parallel processing methods to manage trustworthiness factors, indicators, and levels. Moreover, we would also like to investigate the use of location-based information of mobile learners to our approach, with the aim of improving trustworthiness assessment and then, trustworthiness prediction.

Finally, we discovered that the number of training instances should be increased. Therefore, with the aim of enhancing the prediction model, we plan to modify the learning activity presented in this study in order to generate more training instances. Hence, the student's neural network will be able to accurately predict more trustworthiness different cases (not only those cases with low variation in trustworthiness evolution).

Acknowledgement

This research was partly funded by the Spanish Government through the following projects: TIN2011-27076-C03-02 “CO-PRIVACY”; CONSOLIDER INGENIO 2010 CSD2007-0 004 “ARES”; TIN2013-46181-C2-1-R “COM-MAS” Computational Models and Methods for Massive Structured Data; and TIN2013-45303-P “ICT-FLAG” Enhancing ICT education through Formative assessment, Learning Analytics and Gamification.

References

- [1] T. Koschmann, *Paradigm Shifts and Instructional Technology*, in: T. Koschmann (Ed.), *CSCL: Theory and Practice of an Emerging Paradigm*, Lawrence Erlbaum Associates, Mahwah, New Jersey, 1996, pp. 1–23.
- [2] Z. Luo, T. Zhang, A Mobile Service Platform for Trustworthy E-Learning Service Provisioning, in: S. Caballé, F. Xhafa, T. Daradoumis, A. A. Juan, Z. Luo, T. Zhang (Eds.), *Architectures for Distributed and Complex M-Learning Systems*, IGI Global, 2009, pp. 108–122. URL <http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-60566-882-6>
- [3] S. Caballé, F. Xhafa, L. Barolli, Using mobile devices to support online collaborative learning, *Mob. Inf. Syst.* 6 (1) (2010) 27–47. URL <http://dl.acm.org/citation.cfm?id=1804707.1804710>
- [4] J. Miguel, S. Caballé, J. Prieto, Information Security in Support for Mobile Collaborative Learning, in: *The 7th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2013)*, IEEE Computer Society, Taichung, Taiwan, 2013, pp. 379–384. doi:10.1109/CISIS.2013.69.
- [5] E. R. Weippl, Security in E-Learning, in: H. Bidgoli (Ed.), *Handbook of information security Vol. 1, Key concepts, infrastructure, standards and protocols.*, Vol. 1, Wiley, Hoboken, NJ, 2006, pp. 279–293.
- [6] C. J. Eibl, *Discussion of Information Security in E-Learning*, Ph.D. thesis, Universität Siegen, Siegen, Germany (2010). URL <http://dokumentix.ub.uni-siegen.de/opus/volltexte/2010/444/pdf/eibl.pdf>
- [7] M. J. Dark, *Information assurance and security ethics in complex systems: interdisciplinary perspectives*, Information Science Reference, Hershey, PA, 2011.
- [8] N. H. Mohd Alwi, I.-S. Fan, Information Security Threats Analysis for E-Learning, in: M. D. Lytras, P. Ordonez De Pablos, D. Avison, J. Sipior, Q. Jin, W. Leal, L. Uden, M. Thomas, S. Cervai, D. Horner (Eds.), *Technology Enhanced Learning. Quality of Teaching and Educational Reform*, Vol. 73 of Communications in Computer and Information Science, Springer Berlin Heidelberg, 2010, pp. 285–291, 10.1007/978-3-642-13166-0_41.
- [9] K. M. Apampa, *Presence verification for summative e-assessments*, Ph.D. thesis, University of Southampton, Southampton, England (2010).
- [10] Y. Levy, M. Ramim, A Theoretical Approach For Biometrics Authentication of E-Exams, in: *Chais Conference on Instructional Technologies Research*, The Open University of Israel, Raanana, Israel, 2006, pp. 93–101.
- [11] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, Security in Online Assessments: Towards an Effective Trustworthiness Approach to Support e-Learning Teams, in: *28th International Conference on Advanced Information Networking and Applications (AINA 2014)*, IEEE Computer Society, Victoria, Canada, 2014, pp. 123–130. doi:10.1109/AINA.2014.106.
- [12] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, A Massive Data Processing Approach for Effective Trustworthiness in Online Learning Groups, *Concurrency and Computation: Practice and Experience* doi:10.1002/cpe.3396. URL <http://doi.wiley.com/10.1002/cpe.3396>
- [13] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, L. Barolli, Towards a Normalized Trustworthiness Approach to Enhance Security in On-line Assessment, in: *Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2014)*, IEEE Computer Society, Birmingham, UK, 2014, pp. 147–154. doi:10.1109/CISIS.2014.22.
- [14] J. Miguel, S. Caballé, J. Prieto, Providing Information Security to MOOC: Towards effective student authentication, in: *5-th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2013)*, IEEE Computer Society, Xian, China, 2013, pp. 289 – 292. doi:10.1109/INCoS.2013.52.
- [15] J. D. Demott, A. Sotirov, J. Long, *Gray Hat Hacking, Third Edition Reviews*, 3rd Edition, McGraw-Hill Companies, New York, 2011.
- [16] CSO Magazine, US Secret Service, Software Engineering Insistute CERT Program at Carnegie Mellon University, Deloitte, 2011 *Cybersecurity Watch Survey*, Tech. rep., CSO Magazine (2011).
- [17] Internet Crime Complaint Center, 2013 Internet Crime Report, Tech. rep., Bureau of Justice Assistance (2014). URL <http://www.ic3.gov/media/annualreports.aspx>
- [18] Y. Laouris, N. Eteokleous, We need an Educationally Relevant Definition of Mobile Learning, *Proc mLearn Cape Town* (June) (2005) 1–13.
- [19] D. Gambetta, Can We Trust Trust?, in: *Trust: Making and Breaking Cooperative Relations*, Blackwell, 1988, pp. 213–237.
- [20] Y. Liu, Y. Wu, A Survey on Trust and Trustworthy E-learning System, in: *2010 International Conference on Web Information Systems and Mining*, IEEE, 2010, pp. 118–122. doi:10.1109/WISM.2010.62. URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5662295>
- [21] M. Raza, F. K. Hussain, O. K. Hussain, Neural Network-Based Approach for Predicting Trust Values Based on Non-uniform Input in Mobile Applications, *Comput. J.* 55 (3) (2012) 347–378. doi:10.1093/comjnl/bxr104. URL <http://dx.doi.org/10.1093/comjnl/bxr104>
- [22] S. P. Marsh, *Formalising Trust as a Computational Concept*, Ph.D. thesis, University of Stirling (1994).
- [23] I. Ray, S. Chakraborty, A Vector Model of Trust for Developing Trustworthy Systems, in: D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, P. Samarati, P. Ryan, D. Gollmann, R. Molva (Eds.), *Computer Security – ESORICS 2004*, Vol. 3193, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 260–275.

- [24] S. Msanjila, H. Afsarmanesh, Automating Trust Assessment for Configuration of Temporary Partnerships, in: A. Azevedo (Ed.), *Innovation in Manufacturing Networks*, Vol. 266 of IFIP – The International Federation for Information Processing, Springer US, 2008, pp. 95–104.
- [25] Z. Zhai, W. Zhang, The Estimation of Trustworthy of Grid Services Based on Neural Network, *JNW* 5 (10) (2010) 1135–1142.
URL <http://dblp.uni-trier.de/db/journals/jnw/jnw5.html#ZhaiZ10>
- [26] K. Konrad, G. Fuchs, J. Barthel, Trust and electronic commerce-more than a technical problem, in: *Reliable Distributed Systems*, 1999. Proceedings of the 18th IEEE Symposium on, 1999, pp. 360–365. doi:10.1109/RELDIS.1999.805124.
- [27] W. Song, V. Phoha, X. Xu, An adaptive recommendation trust model in multiagent system, in: *Intelligent Agent Technology*, 2004. (IAT 2004). Proceedings. IEEE/WIC/ACM International Conference on, 2004, pp. 462–465. doi:10.1109/IAT.2004.1342996.
- [28] A. J. Flanagan, M. J. Metzger, Trusting expert- versus user-generated ratings online: The role of information volume, valence, and consumer characteristics, *Computers in Human Behavior* 29 (4) (2013) 1626 – 1634. doi:<http://dx.doi.org/10.1016/j.chb.2013.02.001>.
URL <http://www.sciencedirect.com/science/article/pii/S0747563213000575>
- [29] X. Liu, A. Datta, A Trust Prediction Approach Capturing Agents' Dynamic Behavior, in: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence - Volume Volume Three, IJCAI'11*, AAAI Press, Barcelona, Catalonia, Spain, 2011, pp. 2147–2152. doi:10.5591/978-1-57735-516-8/IJCAI11-358.
URL <http://dx.doi.org/10.5591/978-1-57735-516-8/IJCAI11-358>
- [30] F. Hussain, O. Hussain, E. Chang, Trustworthiness Measurement Methodology (TMM) for Assessment Purposes, in: *Computational Cybernetics*, 2007. ICCCYB 2007. IEEE International Conference on, 2007, pp. 107–112. doi:10.1109/ICCCYB.2007.4402024.
- [31] M. Carbone, M. Nielsen, V. Sassone, A Formal Model for Trust in Dynamic Networks, in: *IN PROC. OF INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING AND FORMAL METHODS (SEFM'03)*, Society Press, 2003, pp. 54–63.
- [32] M. Wojcik, J. Eloff, H. Venter, Trust Model Architecture: Defining Prejudice by Learning, in: S. Fischer-Hübner, S. Furnell, C. Lambri-noudakis (Eds.), *Trust and Privacy in Digital Business*, Vol. 4083 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2006, pp. 182–191.
- [33] P. Laforcade, Towards a UML-based educational modeling language, in: *Advanced Learning Technologies*, 2005. ICALT 2005. Fifth IEEE International Conference on, 2005, pp. 855 – 859. doi:10.1109/ICALT.2005.288.
- [34] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, Security in Online Web Learning Assessment. Providing an Effective Trustworthiness Approach to Support e-Learning Teams, *World Wide Web* (2015) 1–22doi:10.1007/s11280-014-0320-2.
- [35] B. Mobasher, R. Burke, R. Bhaumik, C. Williams, Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness, *ACM Trans. Internet Technol.*doi:10.1145/1278366.1278372.
URL <http://doi.acm.org/10.1145/1278366.1278372>
- [36] B. Aisa, B. Mingus, R. O'Reilly, The Emergent neural modeling system, *Neural Networks* 21 (8) (2008) 1146 – 1152. doi:<http://dx.doi.org/10.1016/j.neunet.2008.06.016>.
URL <http://www.sciencedirect.com/science/article/pii/S0893608008001287>

Computer Standards & Interfaces

Highlights

Manuscript title: A Methodological Approach for Trustworthiness Assessment and Prediction in Mobile Online Collaborative Learning

Keywords: information security; trustworthiness; assessment; prediction; online collaborative learning; mobile learning

Research Highlights:

- Methodology to modelling trustworthiness in mobile online collaborative learning.
- Guidelines for incorporating security into mobile online collaborative activities.
- Provide trustworthiness assessment methods.
- Trustworthiness prediction based on a neuronal network approach.
- Evaluation of trustworthiness prediction and methodology on real online courses.